IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

PORTLAND DIVISION

IN RE: PREMERA BLUE CROSS CUSTOMER DATA SECURITY BREACH LITIGATION	Case No. 3:15-md-2633-SI
This Document Relates to All Actions.	

CASE SUMMARY BRIEF

The Plaintiffs listed in the Table of Related Cases ("Exhibit A") file this case summary brief as requested by the Court's Pretrial Order No. 1. Dkt. No. 7.

I. Factual Background, Allegations, and Claims

Premera Blue Cross ("Defendant" or "Premera") is a Blue Cross Blue Shield affiliate that provides health insurance to subscribers in various states, including Washington and Alaska. Premera is headquartered in Mountlake Terrace, Washington. Defendant is the largest health insurer in Washington and Alaska of both group and individual plans, and administers the Federal Employee Health Benefits ("FEHB") Program, which insures federal employees within those states. Defendant also processes certain claims of subscribers to other Blue Cross Blue Shield affiliates when those out-of-state subscribers seek treatment in Washington or Alaska. As an insurance provider, Premera is a "covered entity" required to comply with the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1986 ("HIPAA"), which sets forth rules governing the privacy and security of health information. Defendant is also bound by the Washington Uniform Health Care Information Act, which also sets forth privacy standards for insurers in Washington. WASH. REV. CODE § 70.02 *et seq.*

In connection with providing insurance services, Defendant requires that subscribers provide it with certain private medical, financial, and personal information. Defendant guarantees the privacy of subscriber information.[1]

[1] For example, Premera's current privacy policy states, "[a]t Premera Blue Cross, we are committed to maintaining the confidentiality of your medical and financial information" and further advises that it "take[s] steps to secure [its] . . . electronic systems from unauthorized access." Premera Blue Cross, Notice of Privacy Policies, Sept. 23, 2013 ver., *at* https://www.premera.com/wa/visitor/privacy-policy/ (last visited July 20, 2015).

A. Premera's Knowledge and Notice of its Security Vulnerabilities

Because Premera administers the FEHB Program, it is subject to routine audits of its data security compliance with HIPAA and industry standard practices. The United States Office of Personnel Management ("OPM") conducted one such audit in early 2014. On April 17, 2014, OPM issued a report to Defendant that identified ten areas of vulnerability in Premera's administrative, electronic, and computer security systems and made recommendations for immediate remediation to secure the systems and data. Among other things, OPM determined that Premera was not in compliance with many industry standards that ensure private data security.

In connection with the audit, OPM identified several specific vulnerabilities and deficiencies. Among them, OPM determined that Premera routinely failed to promptly install updates and security patches to network systems, which created a risk of hackers breaching sensitive private information. OPM also reported that Premera used several types of out-of-date software, some of which had known security vulnerabilities and were no longer supported by their vendors. OPM warned that Premera's use of this out-of-date software exposed its systems and data to vulnerabilities including "malicious code such as viruses and worms" or "malware"—vulnerabilities that could be exposed by hackers and used to compromise Premera's systems and the personal, financial, and medical information of its subscribers. Furthermore, OPM warned Premera that its operating systems were insecurely configured and that this could enable hackers or unprivileged users to infiltrate Premera's computer systems, escalate their privileges, and use those privileges to obtain a host of sensitive, proprietary, and confidential information. Premera received and reviewed this report. Rather than immediately addressing the vulnerabilities identified, Premera instead responded that it would investigate and remediate

any deficiencies in its computer systems by December 31, 2014, over eight months after the OPM audit and resulting report.

B. Hackers Take Advantage of Premera's Security Vulnerabilities and Initiate a Malware Attack that Lasts at Least Eight Months

On or about May 5, 2014, weeks after Premera received the OPM audit report containing warnings about its serious vulnerability to outside attack, hackers installed malware on Premera's systems and used it to access private medical records, including clinical data, sensitive health information, subscriber names, birthdays, addresses, e-mails, telephone numbers, Social Security numbers, and bank account information (the "Compromised Data"). According to Premera, the malware remained active on its computer systems for over eight months. In or around January 2015, Premera reportedly detected the malware and allegedly took steps to eliminate it from its systems and stop the breach and exposure of the Compromised Data. Before then, the private medical, financial, and personal data of 11 million people, including all Premera Blue Cross subscribers from 2002 through at least January 2015 and all non-Premera, Blue Cross insured patients who sought medical or clinical treatment in Washington or Alaska during the same time period, was exposed to cyber criminals and hackers.

Despite knowing that its subscribers' personal and private information was exposed, published, and compromised since at least January 2015, Premera did nothing to inform those victims affected by the breach until March 2015. From May 2014 through March 2015, while Premera stood by without addressing these problems, hackers used the private information of a number of plaintiffs and proposed class members to open fraudulent accounts, file fraudulent tax returns, and steal their identities.

Plaintiffs and members of the proposed class, in connection with their health care, used Defendant's services and provided Premera with their medical, financial, and personal private

information in exchange for assurances by Premera that the information would remain secure and confidential. However, Premera failed to meet the required standard of care in safeguarding Plaintiffs' and class members' medical, financial, and personal information. For months, Premera did nothing to eliminate the data-breach-causing malware and continued to expose the medical, financial, and personal information of Plaintiffs and class members long after it knew or should have known that its systems were infected. This failure resulted in long-term exposure of the Compromised Data to hackers and other criminals. Premera also failed to disclose to Plaintiffs and members of the proposed class that its computer systems and security practices were inadequate to reasonably safeguard their medical, financial, and personal information.

C. The Stolen Medical, Financial, and Personal Data is Extremely Valuable on the Cyber Black Market

The compromised subscriber data is very valuable to cyber criminals. As the Federal Trade Commission recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[2] Some cybersecurity experts estimate that medical data—like that stolen from Premera—is worth at least 10 times that of credit card data on the black market.[3] At a December 1, 2011 panel of cybersecurity experts, the panel estimated that a single person's medical record was worth approximately $50 on the cyber black market.[4] The other data

[2] Federal Trade Commission, Warning Signs of Identity Theft, http://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft.

[3] Sometimes, medical records are worth significantly more. *See* Aarti Shahani, *The Black Market for Stolen Health Care Data*, NPR.ORG, Feb. 13, 2015, http://www.npr.org/sections/alltechconsidered/2015/02/13/385901377/the-black-market-for-stolen-health-care-data (noting that a reporter found a set of 10 Medicare records selling for 22 bitcoins, or $4,700 at that day's exchange rate).

[4] Robert Lowes, *Stolen EHR Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM, Apr. 28, 2014, http://www.medscape.com/viewarticle/824192.

released in this data breach, such as name, address, Social Security number, and birth date have a significant monetary value as well. Accordingly, the total value of the data maintained by Premera and exposed, released, and published in this breach amounts to at least hundreds of millions of dollars.

The ramifications of Premera's data breach are severe and long-lasting. The exposure of medical records is of particular concern to victims, as medical records contain the victims' most private information. According to a 2013 study by data security experts, one out of four data breach notification recipients in 2012 became a victim of identity fraud.[5] Unlike a credit card that can be canceled when someone learns their data has been stolen, much of the information stolen in the Premera data breach, such as medical records, Social Security numbers, address history, and birth dates are impossible or nearly impossible to change[6], and victims of Premera's data breach will be affected for years to come, if not for the rest of their lives.

D. Premera's Post-Breach Conduct

Premera offered all victims two years of free credit monitoring and identity theft protection services. Unfortunately, identity thieves often sit on stolen information for years before attempting to use it. Indeed, Premera concedes that "identity theft can happen months and even years after a data breach."[7] On July 14, 2015, the Blue Cross Blue Shield Association

[5] https://www.javelinstrategy.com/news/1387/92/More-Than-12-Million-Identity-Fraud-Victims-in-2012-According-to-Latest-Javelin-Strategy-Research-Report/d,pressRoomDetail.

[6] A victim of identity theft can only petition to change their Social Security number by showing that the victim "continues to be disadvantaged by using the original number." https://faq.ssa.gov/link/portal/34011/34019/Article/3789/Can-I-change-my-Social-Security-number. Changing a Social Security number has additional consequence for victims' credit history, ability to obtain credit, and may create background check complications, among other issues.

[7] http://www.premeraupdate.com/free-credit-monitoring/ (visited July 20, 2015).

announced that beginning January 1, 2016, it would offer credit monitoring, fraud detection services, and fraud resolution support to all subscribers nationwide.[8] This announcement fails to provide any details of the promised services; however, the services clearly do not include identity theft insurance or any proactive solutions.

E. Claims in the Multi District Litigation

Plaintiffs in the various cases have pled several causes of action on behalf of a proposed nationwide class under Washington law, or alternatively, state-specific subclasses. The key claims in the lawsuit are for violation of the Washington data breach notification law, and state consumer protection, negligence, breach of contract, breach of fiduciary duty, unjust enrichment, and common law invasion of privacy laws. The critical legal issues likely to be presented include whether Plaintiffs have Article III and statutory standing; whether Defendant breached its duty of care, whether Defendant violated HIPAA or the Washington Uniform Health Care Information Act; whether nationwide or state-specific classes are appropriate; whether Defendant breached its duty to Plaintiffs resulting in the data breach; whether Defendant is liable to victims to remediate its breach of duty; whether Defendant is contractually obligated to adhere to best practices for data security; whether Defendant is contractually obligated to secure Plaintiffs' medical, financial, and personal information; and the appropriate measure of damages and/or equitable relief to be awarded to Plaintiffs and class members.

II. Procedural Status of Cases

All of the related cases before the Honorable Ricardo S. Martinez were stayed pending the Judicial Panel on Multidistrict Litigation's ("JPML's") transfer decision. *See, e.g., Webb v.*

---

[8] Press Release, July 14, 2015, *at* http://www.bcbs.com/healthcare-news/bcbsa/bcbsa-announces-new-identity-protection-services-for-customers-nationwide.html.

Premera Blue Cross, No. 3:15-cv-01156 (D. Or.), Dkt. No. 4, (order staying case). Four cases were not stayed prior to this Court's Pretrial Order No. 1, Dkt. No. 7. *See Eykel v. Premera Blue Cross*, No. 3:15-cv-01169-SI (D. Or.); *Fuerst v. Premera Blue Cross*, No. 3:15-cv-01170-SI (D. Or.); *Kaihoi v. Premera et al.*, No. 3:15-cv-01171-SI (D. Or); and *Dudley v. Premera Blue Cross*, No. 3:15-cv-01172-SI (D. Or.). In *Dudley*, a motion for protective order to preserve evidence was filed on May 11, 2015 and denied on May 26, 2015. No. 3:15-cv-01172-SI (D. Or.), at Dkt. Nos. 3, 5. To the best of Plaintiffs' knowledge, discovery has not commenced in any of the related cases. Premera has not answered or filed any motions in response to any of the complaints. During a July 27, 2015 meet and confer call with Defendant, defense counsel advised that Premera is awaiting the appointment of lead counsel to discuss all discovery issues, including a protective order and ESI protocol.

III. Status of Related State Court Litigation

Defense counsel has confirmed that there are no related proceedings pending in any state courts. On April 8, 2015, *Welch v. Premera*, No. 3:15-cv-01158-SI (filed Mar. 30, 2015, No. 15-2-07774-1) was removed from King County Superior Court in Washington and is currently pending before this Court.

IV. Predicted Total Number of Cases

To date, thirty-four filed cases have been transferred to this Court by the JPML. In addition, five cases were filed in and are currently pending in this District. There are currently no cases awaiting transfer by the JPML. The only additional cases filed this month were filed by counsel already appearing in the litigation. It is unlikely that many, if any, additional cases will be filed given the status of the litigation, especially once lead counsel is appointed.

DATED: July 31, 2015

Respectfully submitted,

/s/ Keith S. Dubanevich

Keith S. Dubanevich, OSB No. 975200
Steve D. Larson, OSB No. 863540
Mark A. Friel, OSB No. 002592
STOLL STOLL BERNE LOKTING & SHLACHTER P.C.
209 SW Oak St., Suite 500
Portland, OR 97204
Tel: (503) 227-1600
Fax: (503) 227-6840
Email: slarson@stollberne.com
mfriel@stollberne.com
kdubanevich@stollberne.com

Proposed Interim Liaison Counsel

Bryan L. Clobes
Kelly L. Tucker
Cafferty Clobes Meriwether & Sprengel, LLP
1101 Market St., Suite 2650
Philadelphia, PA 19107
Tel: (215) 864-2800
Fax: (215) 864-2810
Email: bclobes@caffertyclobes.com
ktucker@caffertyclobes.com

Jennifer Winter Sprengel
Nyran Rose Rasche
Cafferty Clobes Meriwether & Sprengel LLP
150. S. Wacker
Suite 3000
Chicago, IL 60606
Tel: (312) 782-4880
Fax: (312) 782-4485
Email: jsprengel@caffertyclobes.com
nrasche@caffertyclobes.com

Proposed Interim Lead Counsel

This brief is also joined by the following:

Vincent J. Esades
HEINS MILLS & OLSON, P.L.C.
310 Clifton Avenue
Minneapolis, MN 55403
Telephone: (612) 338-4605
Facsimile: (612) 338-4692
Email: vesades@heinsmills.com

Joseph G. Sauder
Chimicles & Tikellis LLP
361 West Lancaster Avenue
Haverford, PA 19041
610-642-8800
Fax: 610-649-3633
jgs@chimicles.com

Robert S. Schachter
Sona R. Shah
ZWERLING, SCHACHTER & ZWERLING, LLP
41 Madison Avenue, 32nd Floor
New York, NY 10010
Telephone: (212) 223-3900
Facsimile: (212) 371-5969
rschachter@zsz.com
sshah@zsz.com

Dan Drachler (WSBA #27728)
ZWERLING, SCHACHTER & ZWERLING, LLP
1904 Third Avenue, Suite 1030
Seattle, WA 98101-1170
Telephone: (206) 223-2053
Facsimile: (206) 343-9636
ddrachler@zsz.com

Mark S. Goldman
Paul J. Scarlato
Brian D. Penny
GOLDMAN SCARLATO & PENNY, PC
101 E. Lancaster Avenue, Suite 204
Wayne, PA 19087
Telephone: (484) 342-0700
Facsimile: (484) 580-8747
Email: goldman@lawgsp.com
scarlato@lawgsp.com
penny@lawgsp.com

Stephen R. Basser
Jeffrey Golan
BARRACK RODOS & BACINE
600 W. Broadway
Ste. 1700
San Diego, CA 92101
619−230−0800
sbasser@barrack.com
jgolan@barrack.com

Irwin B. Levin
Richard E. Shevitz
Lynn A. Toops
COHEN & MALAD, LLP
One Indiana Square, Ste. 1400
Indianapolis, IN 46204
Telephone: (317) 636-6481
Facsimile: (317) 636-2495
ilevin@cohenandmalad.com
rshevitz@cohenandmalad.com
ltoops@cohenandmalad.com

Harris L. Pogust
Kevin O'Brien
Pogust Braslow & Millrood, LLC
161 Washington St., Suite 1520
Conshohocken, PA 19428
Tel: (610) 941-4204
Fax: (610) 941-4248
Email: hpogust@pbmattorneys.com
kobrien@pbmattorneys.com

John G. Emerson
EMERSON POYNTER LLP
830 Apollo Lane
Houston, TX 77058-2610
Telephone: (281) 488-8854
Facsimile: (281) 488-8867
Email: jemerson@emersonpoynter.com

Scott E. Poynter
Will T. Crowder
EMERSON POYNTER LLP
1301 Scott Street
Little Rock, AR 72202
Telephone: (501) 907-2555
Facsimile: (501) 907-2556
Email: scott@emersonpoynter.com
Email: wcrowder@emersonpoynter.com

Cliff Cantor
Law Offices of Clifford A. Cantor, P.C.
627 208th Ave. SE
Sammamish, WA 98074
Tel: (425) 868-7813
Fax: (425) 732-3752
Email: cliff.cantor@outlook.com

Daniel A. Rogers
Duncan Calvert Turner
Badgley Mullins Turner PLLC
19929 Ballinger Way NE, Ste. 200
Seattle, WA 98155
206−621−6566
drogers@badgleymullins.com
dturner@badgleymullins.com

Attorneys for Plaintiffs